UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/887,776	06/21/2001	Philip Zimmermann	002.0218.01	9088

23419 7590 03/25/2004

COOLEY GODWARD, LLP
3000 EL CAMINO REAL
5 PALO ALTO SQUARE
PALO ALTO, CA 94306

EXAMINER	
SONG, HOSUK	

ART UNIT	PAPER NUMBER
2135	5

DATE MAILED: 03/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/887,776	Applicant(s) ZIMMERMANN, PHILIP	
	Examiner Hosuk Song	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *6/21/20001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-16,18-27,29-35 and 37-43* is/are rejected.

7)☒ Claim(s) *7,17,28 and 36* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-6,8-16,18-27,29-35,37-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas et al.(US 5,200,999) in view of Lipner et al.(US 5,557,765).

Claims 1,10: Matyas discloses generating a first key pair for a user, comprising a public key employed for encrypting message to the user and comprising a private key employed for decrypting messages which have been encrypted using the public key of the first key pair in (col.22,lines 40-45,53-55). Matyas discloses generating a second key pair in (col.10,lines 50-61). Matyas discloses information referencing the public key of the second key pair embedded within the public key of the first key pair in (col.12,lines 28-53). Matyas discloses an encryption module automatically employing the public key of the second key pair during encryption of the message under the public key of the first key pair so that the message being encrypted can be directly decrypted using the private key of the second key pair in (col.26,lines 29-53). Matyas does not specifically disclose second key pair comprising a public key employed for recovering messages. Lipner's patent discloses message recovery using a second key pair in (fig.8,#820 and col.10,lines 33-44). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ message recovery scheme by a second key pair as taught in Lipner with key generation and encryption method disclosed in Matyas in order to safely recover or retrieve data which has been encrypted or misplaced. It allows for safe means to

manage its data against hackers. Further, since there is a second key pair involved it adds extra level of security such that hackers must go first through first key pair before accessing second key pair.

Claim 2: Matyas disclose information which uniquely identifies the public key of the second pair stored into the public key of the first key pair in (col.12,lines 12-27).

Claim 3: Matyas discloses a copy of the public key of the second key pair includes information pointing to a location where the second key pair is stored in (col.24,lines 48-59).

Claim 4: Matyas discloses a copy of the public key of the second key pair embedded within the public key of the first key pair in (col.24,lines 43-59).

Claim 5: Matyas does not specifically disclose a pointer which uniquely identifies the public key of the second pair. Official notice is taken that using a pointer is well known in the art. One of ordinary skill in the art would have been motivated to use pointer in order to quickly identify,locate and retrieve data from storage.

Claim 6: Matyas discloses constraints specifying use of the public key of the first pair in (col.7,lines 20-40).

Claim 8: Matyas does not specifically disclose Diffie-Hellman compatible key pair. Official notice is taken that Diffie-Hellman key pair is well known in the art. One of ordinary skill in the art would have been motivated to employ Diffie-Hellman because DH effectively provides effective and secure means for key distribution and key generation.

Claim 9: Matyas discloses RSA compatible key pair in (col.7,lines 2-34).

Claims 11,20: Matyas discloses generating a first key pair for a user, comprising a public key employed for encrypting message to the user and comprising a private key employed for decrypting messages which have been encrypted using the public key of the first key pair in (col.22,lines 40-45,53-55). Matyas discloses generating a second key pair in (col.10,lines 50-

61). Matyas discloses information referencing the public key of the second key pair embedded within the public key of the first key pair in (col.12,lines 28-53). Matyas discloses an encryption module automatically employing the public key of the second key pair during encryption of the message under the public key of the first key pair so that the message being encrypted can be directly decrypted using the private key of the second key pair in (col.26,lines 29-53). Matyas does not specifically disclose second key pair comprising a public key employed for recovering messages. Lipner's patent discloses message recovery using a second key pair in (fig.8,#820 and col.10,lines 33-44). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ message recovery scheme by a second key pair as taught in Lipner with key generation and encryption method disclosed in Matyas in order to safely recover or retrieve data which has been encrypted or misplaced. It allows for safe means to manage its data against hackers. Further, since there is a second key pair involved it adds extra level of security such that hackers must go first through first key pair before accessing second key pair.

Claim 12: Matyas disclose information which uniquely identifies the public key of the second pair in (col.12,lines 12-27).

Claim 13: Matyas discloses a copy of the public key of the second key pair includes information pointing to a location where the second key pair is stored in (col.24,lines 48-59).

Claim 14: Matyas discloses a copy of the public key of the second key pair embedded within the public key of the first key pair in (col.24,lines 43-59).

Claim 15: Matyas does not specifically disclose a pointer which uniquely identifies the public key of the second pair. Official notice is taken that using a pointer is well known in the art. One of ordinary skill in the art would have been motivated to use pointer in order to quickly identify,locate and retrieve data from storage.

Claim 16: Matyas discloses constraints specifying use of the public key of the first pair in (col.7,lines 20-40).

Claim 18: Matyas does not specifically disclose Diffie-Hellman compatible key pair. Official notice is taken that Diffie-Hellman key pair is well known in the art. One of ordinary skill in the art would have been motivated to employ Diffie-Hellman because DH effectively provides effective and secure means for key distribution and key generation.

Claim 19: Matyas discloses RSA compatible key pair in (col.7,lines 2-34).

Claim 21: Matyas discloses storage medium for holding for performing function in (fig.1,13).

Claims 22-26,29: Matyas discloses CBC in (col.22,lines 59-63). Matyas does not specifically disclose a session encryption module block-cipher encrypting a plaintext message into cipher text using a session key. It would have been obvious to person of ordinary skill in the art at the time invention was made to employ session key as taught in Lipner with CBC disclosed in Matyas because session has short lifetime span, keys are protected against repeated and random attacks. Matyas does not specifically disclose second key pair comprising a public key employed for recovering messages. Lipner's patent discloses message recovery using a second key pair in (fig.8,#820 and col.10,lines 33-44). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ message recovery scheme by a second key pair as taught in Lipner with key generation and encryption method disclosed in Matyas in order to safely recover or retrieve data which has been encrypted or misplaced. It allows for safe means to manage its data against hackers. Further, since there is a second key pair involved it adds extra level of security such that hackers must go first through first key pair before accessing second key pair.

Claim 27: Mayas does not specifically disclose a pointer which uniquely identifies the public key of the second pair. Official notice is taken that using a pointer is well known in the art. One of ordinary skill in the art would have been motivated to use pointer in order to quickly identify,locate and retrieve data from storage.

Claim 30-37: Matyas discloses CBC in (col.22,lines 59-63). Matyas does not specifically disclose a session encryption module block-cipher encrypting a plaintext message into cipher text using a session key. It would have been obvious to person of ordinary skill in the art at the time invention was made to employ session key as taught in Lipner with CBC disclosed in Matyas because session has short lifetime span, keys are protected against repeated and random attacks. Matyas does not specifically disclose second key pair comprising a public key employed for recovering messages. Lipner's patent discloses message recovery using a second key pair in (fig.8,#820 and col.10,lines 33-44). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ message recovery scheme by a second key pair as taught in Lipner with key generation and encryption method disclosed in Matyas in order to safely recover or retrieve data which has been encrypted or misplaced. It allows for safe means to manage its data against hackers. Further, since there is a second key pair involved it adds extra level of security such that hackers must go first through first key pair before accessing second key pair.

Claim 38: Matyas discloses medium in (fig.1,13).

Claims 39-42: Matyas discloses CBC in (col.22,lines 59-63). Matyas does not specifically disclose a session encryption module block-cipher encrypting a plaintext message into cipher text using a session key. It would have been obvious to person of ordinary skill in the art at the time invention was made to employ session key as taught in Lipner with CBC disclosed in Matyas because session has short lifetime span, keys are protected against

repeated and random attacks. Matyas does not specifically disclose second key pair comprising a public key employed for recovering messages. Lipner's patent discloses message recovery using a second key pair in (fig.8,#820 and col.10,lines 33-44). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ message recovery scheme by a second key pair as taught in Lipner with key generation and encryption method disclosed in Matyas in order to safely recover or retrieve data which has been encrypted or misplaced. It allows for safe means to manage its data against hackers. Further, since there is a second key pair involved it adds extra level of security such that hackers must go first through first key pair before accessing second key pair.

Claim 43: Matyas discloses medium in (fig.1,13).

Allowable Subject Matter

2. Claims 7,17,28,36 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 7,17: Prior art of record does not teach constraints include a constraints include a constraint specifying that use of the public of the second key pair is mandatory during encryption of a message using the public key of the first key pair.

Claims 28,36: Prior art of record does not teach at least one of a cryptographic and a message digest of the pointer stored as the reference to the public key of the message recovery agent.

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Bruce Schneier (Applied Cryptography) discloses CBC and Diffie-Hellman key exchange.

b. Tysen et al.(US 5,497,422) discloses public key cryptosystem with message digest.

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hosuk Song whose telephone number is 703-305-0042. The examiner can normally be reached on Tue-Fri 6:00 am-4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HS